SWA Access to SSA Data
through the Interstate Connection Network
IV&V Specifications

3/17/2004

Table of Contents

SWA Access to SSA Data
Through the Interstate Connection Network
IV&V Specifications

1.0 Purpose

The purpose of this document is to describe the requirements for verifying SWA compliance with the Social Security Administration's systems security requirements for connecting to SSA's Unemployment Insurance Query program through the ICON. Each SWA that implements the online connection to SSA through ICON must have an independent certification performed by a professional auditor that offers Independent Verification and Validation (IV&V) services. SWA's must obtain this systems security compliance certification prior to being authorized by DOL to access SSA information through the ICON. Additionally, a DOL official will use this document, as a guide, when evaluating and certifying the SWAs' system design.

SWAs must first negotiate a data sharing agreement with SSA before a systems security certification and compliance review can be conducted by an IV&V contractor. Following initial systems security compliance certification through this process, SSA will monitor ongoing SWA compliance with their systems security requirements through its own periodic onsite reviews.

2.0 Background

SSA is required by law to protect personal information from unauthorized use or disclosure. The Director, SSA Office of Systems Security Operations Management is responsible for assuring that external systems that receive information from SSA are secure and operate in a manner that is consistent with SSA's own systems security policies, and are in compliance with the terms of information sharing agreements executed by SSA. Normally, in carrying out this responsibility, SSA requires data exchange partners who request online access to submit written documentation of their system design and security features, and then SSA conducts onsite verification prior to allowing the exchange partner to access information from SSA. For the purpose of facilitating SWA access to SSA information through the ICON, DOL has agreed to take on this responsibility and certify that SWA's have complied with SSA's systems requirements.

3.0 SWA System Security Certification Review

Each state must have a systems security certification review completed by an independent third-party and be "certified" as meeting the SSA security requirements before they can connect to SSA's UIQ program through ICON. The reviewer must be a qualified vendor or accredited auditor offering IV&V services for information systems including technological systems security applications and procedures.

The required systems security certification review will consist of an onsite inspection of the SWA's client support system and data center to observe physical security safeguards, a demonstration of the implementation of the UIQ connectivity to the SSA information, and discussion of each of these requirements with the SWA's responsible management personnel. The reviewer also will request a demonstration of the SWA's audit trail capability and will visit at least one of the SWA's field offices to review the SWA's implementation of systems security awareness procedures and procedures regarding the proper handling and protection of SSA-supplied information with workers and managers.

The following section describes the steps that must be performed in order to certify that the SWA meets the SSA systems security requirements for online access, as specified above in section 3.

Note: All references to written documentation can be taken to mean either hardcopy or online documentation, unless specified otherwise. Where written signatures are required, document imaging systems may be used to retain copies of signed documents, or digital signatures may be employed where authorized by state law or Federal laws where applicable.)

3.1 Review of System Design Documentation

The IV&V contractor will verify that the SWA has submitted to DOL written systems security documentation conforming to SSA requirements. DOL will provide a copy of this documentation to the contractor in advance of the scheduled onsite review of the SWA.

The SWA documentation that the IV&V contractor will use as the basis for their verification and validation review will consist of the documentation specified in the *Systems Security Requirements for SWA Access to SSA Information Through the ICON System* which is attached to the individual data exchange agreements between SWA's and SSA. A copy of this document also is attached to this document at Appendix A.

The IV&V contractor will verify and certify in their report that the SWA's system design documentation addresses each of the SSA system security requirements as specified in SSA's requirements document.

3.2 Automated Audit Trail

- The IV&V contractor will verify and certify in their report that the SWA has an audit trail system
- The reviewer, with the assistance of SWA personnel, will verify that the audit trail capability conforms to SSA requirements, and is able to:

  a. Identify the SWA employee who initiated the online query request for SSA information, or the SWA client case associated with the transaction if the query is systems generated.

b. Identify the time and date of the request, as well as

c. Identify the client case related to the transaction.

3.3 System Access Control

- The IV&V contractor will verify and certify in their report that the SWA's system access control process and infrastructure conforms to SSA requirements. The reviewer will meet with the individual(s) responsible for System Access Control functions and observe a demonstration of the procedures for logging onto the system for accessing SSA information through the online query.
- The reviewer will verify that a written description of the SWA's Data Exchange technological access controls has been created. The document must:

    a. Identify the type of software used. If commercial packages are employed, or authentication/access control features of common operating systems are used (e.g., Windows or UNIX user accounts coupled with various types of group access), the version and maintenance level should be documented. If custom software is specified, identify the developer or vendor and provide the user documentation for review.

    b. Provide an overview of the process used to grant access to protected information for workers in different job categories, and

    c. Provide a written description of the function responsible for PIN/password issuance and maintenance.

- The reviewer will verify that the SWA's system access control uses a recognized user access security software package (e.g. RAC-F, ACF-2, and TOP SECRET) or an equivalent security software design. Where access to a mainframe is required as part of the UIQ, verification will include a demonstration of RACF authentication/authorization using a valid password, as well as demonstration of logon failure when incorrect passwords are provided.
- The reviewer will verify that the access control software utilizes personal identification numbers (PIN) and passwords (or biometric identifiers) in combination with the user's system identification code. System verification will include a demonstration showing that two-factor authentication (e.g., PIN/Password or PIN/Biometric identifier) allows access the UIQ system, as well as demonstrating that invalid credentials will cause logon failure.
- The reviewer will verify that the SWA has management controls and oversight of the function of issuing and maintaining access control PINs and passwords ensuring only authorized users have access to UIQ. Verification will consist of reviewing the written procedures that cover the process.

3.4 Monitoring and Anomaly Detection

- The reviewer will verify that the SWA's system design for online access to SSA information includes monitoring and anomaly detection capabilities to deter employees from browsing unauthorized information.

  An illegal access, "accessing SSA records not associated with a UI claim", will be attempted and verification will determine whether appropriate actions are initiated by the system (i.e., logging, access denial).

- The reviewer will verify that the SWA's system design can produce reports indicating the capability to appropriately monitor user access. Legal and illegal accesses will be performed and the ensuing reports will be examined for expected results.
- The reviewer will review the reports for content appropriateness based upon the report type, such as:

  a. *User ID exception reports*

  This type of report captures information about users who enter incorrect user ID's when attempting to gain access to the system, including failed attempts to enter a password.

  b. *Inquiry match exception reports*

  This type of report captures information about users who may be initiating UIQ transactions for Social Security Numbers that have no client case association within the outside entity's system.

  c. *System error exception reports*

  This type of report captures information about users who may not understand or be following proper procedures for UIQ access.

  d. *Inquiry activity statistical reports*

  This type of report captures information about UIQ usage patterns among authorized users.

- The reviewer will also meet with SWA employees responsible for reviewing such reports. Documented procedures for reviewing both standard and exception reports will be examined, individual responsible for conducting the review will be identified and documented methods for tracking problems identified by reports will be reviewed.
- The reviewer will certify that the SWA has anomaly detection procedures for the SWA's employees responsible for reviewing the reports, addressed above. Anomaly reports will be reviewed for ease of use. Written procedures for distributing reports

and assigning responsibility will be reviewed. If anomalies are buried in general log files, methods employed to facilitate exception handling will be demonstrated by the reviewers to verify that anomalies can be readily identified.

3.5 Management Oversight and Quality Assurance

- The reviewer will verify that the SWA has established ongoing management oversight and quality assurance capabilities for monitoring the issuance and maintenance of user ID's for online access to SSA information. Verification will include the review of documented procedures, as well as a review of a log or other method used to control issuance of access to the UIQ system.
- When certifying the SWA's system, SSA will meet with the individuals responsible for these functions and request a description of how these responsibilities are carried out.

3.6 Security Awareness and Employee Sanctions

- The reviewer will verify that the SWA is providing security awareness training for employees. Verification will include documented training schedules or procedures. The period examined will include the previous year and plans for the following year. Records that are used to verify that employees have received appropriate training will be examined.
- The reviewer will verify that the security awareness training provided includes information about the SWA's responsibility for:

    a. Proper use

    b. Proper protection of SSA information, and

    c. Possible sanctions for misuse of online access to SSA information.

    Verification will include a review of the training materials.
- The reviewer will obtain information on how these functions will be performed within the SWA's organization, identifying the individual(s) or component(s) responsible for performing the functions. Verification will determine that an individual or the department has been assigned responsibility for the training, and that training has been conducted in accordance with a documented plan.
- Additionally, the reviewer will meet with the individuals responsible for these functions and request a written description of how these responsibilities are carried out.

3.7 After certification and Periodic Certification Review(s)

- After certification and upon network connectivity to the SSA UIQ, the reviewer will perform a follow-up certification review after live transmission of SSA online information to the SWA. The reviewer will verify the automated audit trail capability by asking the SWA to retrieve audit trail information for a sample of live transactions received by SSA. The information submitted to the reviewer, in support of the sample transactions, must be certified as accurate by an appropriate management official of the SWA.

4.0 SWA Certification submission to DOL

Generally, the certification review will address each of the requirements described above and will include, where appropriate, a demonstration report of the SWA's implementation of each requirement. The reviewer must certify that the SWA system design for online access to SSA information includes all security elements as required by SSA.

4.1 Initial Determination

- Following a successful security certification review, the reviewer will submit an initial determination certification report to DOL as well as the SWA.
- DOL will have 21 working days to respond to the initial determination certification review report.

4.2 Final Determination

- The reviewer will address each comment of the initial determination and submit a final determination certification report to DOL.

No specific format for submitting this information is required. However, regardless of how it is presented, the initial determination and final determination document should be submitted covering each of the items in section 3.0, above, over the signature of an official representative of the SWA.

APPENDIX A

Systems Security Requirements for SWA Access to
SSA Information through the ICON System

A. General Systems Security Standards

SWA's that request and receive information from SSA through the ICON system must comply with the following general systems security standards concerning access to and control of SSA information. The SWA must restrict access to the information to authorized employees who need it to perform their official duties. Similar to IRS requirements, information retrieved from SSA must be stored in a manner that is physically and electronically secure from access by unauthorized persons during both duty and non-duty hours, or when not in use. SSA information must be processed under the immediate supervision and control of authorized personnel. The SWA must employ both physical and electronic safeguards to ensure that unauthorized personnel cannot retrieve SSA information by means of computer, remote terminal or other means.

All persons who will have access to any SSA information must be advised of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal and State laws. SSA may, at its discretion, make on-site inspections or other provisions to ensure that adequate safeguards are being maintained by the SWA.

B. System Security Requirements for SWA's

SWA's that receive SSA information through the ICON system must comply with the following systems security requirements which must be met before DOL will approve a request from an SWA for online access to SSA information through the ICON system. The SWA system security design and procedures must conform to these requirements. They must be documented by the SWA and subsequently certified by either DOL or by an Independent Verification and Validation (IV&V) contractor prior to initiating transactions to and from SSA through the ICON.

No specific format for submitting this documentation to DOL is required. However, regardless of how it is presented, the information should be submitted to DOL in both hardcopy and electronic format, and the hardcopy should be submitted over the signature of an official representative of the SWA. Written documentation should address each of the following security control areas:

1. General System Security Design and Operating Environment

The SWA must provide a written description of its system configuration and security features. This should include the following:

a. A general description of the major hardware, software and communications platforms currently in use, including a description of the system's security design features and user access controls; and

b. A description of how SSA information will be obtained by and presented to SWA users, including sample computer screen presentation formats and an explanation of whether the SWA system will request information from SSA by means of systems generated or user initiated transactions; and

c. A description of the organizational structure and relationships between systems managers, systems security personnel, and users, including an estimate of the number of users that will have access to SSA data within the SWA system and an explanation of their job descriptions.

Meeting this Requirement

SWA's must explain in their documentation the overall design and security features of their system. During onsite certification, the IV&V contractor, or other certifier, will use the SWA's design documentation and discussion of the additional systems security requirements (following) as their guide for conducting the onsite certification and for verifying that the SWA systems and procedures conform to SSA requirements.

Following submission to the DOL in connection with the initial certification process, the documentation must be updated any time significant architectural changes are made to the system or to its' security features. During its future compliance reviews (see below), the SSA will ask to review the updated design documentation as needed.

2. Automated Audit Trail

SWA's receiving SSA information through the ICON system must implement and maintain a fully automated audit trail system capable of data collection, data retrieval and data storage. At a minimum, data collected through the audit trail system must associate each query transaction to its initiator and relevant business purpose (i.e. the SWA client record for which SSA data was requested), and each transaction must be time and date stamped. Each query transaction must be stored in the audit file as a separate record, not overlaid by subsequent query transactions.

Access to the audit file must be restricted to authorized users with a "need to know" and audit file data must be unalterable (read only) and maintained for a minimum of three (preferably seven) years. Retrieval of information from the automated audit trail may be accomplished online or through batch access. This requirement must be met before DOL

will approve the SWA's request for access to SSA information through the ICON system.

If SSA-supplied information is retained in the SWA system, or if certain data elements within the SWA system will indicate to users that the information has been verified by SSA, the SWA system also must capture an audit trail record of any user who views SSA information stored within the SWA system. The audit trail requirements for these inquiry transactions are the same as those outlined above for SWA transactions requesting information directly from SSA.

Meeting this Requirement

The SWA must include in their documentation a description of their audit trail capability and a discussion of how it conforms to SSA's requirements. During onsite certification, the IV&V contractor, or other certifier, will request a demonstration of the system's audit trail and retrieval capability. The SWA must be able to identify employee's who initiate online requests for SSA information (or, for systems generated transaction designs, the SWA case that triggered the transaction), the time and date of the request, and the purpose for which the transaction was originated. The certifier, or IV&V contractor, also will request a demonstration of the system's audit trail capability for tracking the activity of SWA employees that are permitted to view SSA supplied information within the SWA system, if applicable.

During its future compliance reviews (see below), the SSA also will test the SWA audit trail capability by requesting verification of a sample of transactions it has processed from the SWA after implementation of access to SSA information through the ICON system.

3. System Access Control

The SWA must utilize and maintain technological (logical) access controls that limit access to SSA information to only those users authorized for such access based on their official duties. The SWA must use a recognized user access security software package (e.g. RAC-F, ACF-2, TOP SECRET) or an equivalent security software design. The access control software must utilize personal identification numbers (PIN) and passwords (or biometric identifiers) in combination with the user's system identification code. The SWA must have management control and oversight of the function of authorizing individual user access to SSA information, and over the process of issuing and maintaining access control PINs and passwords for access to the SWA system.

Meeting this Requirement

The SWA must include in their documentation a description of their technological access controls, including identifying the type of software used, an overview of the process used to grant access to protected information for workers in different job categories, and a description of the function responsible for PIN/password issuance and maintenance.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individual(s) responsible for these functions to verify their responsibilities in the SWA's access control process and will observe a demonstration of the procedures for logging onto the SWA system and for accessing SSA information.

4. Monitoring and Anomaly Detection

The SWA's system must include the capability to prevent employees from browsing (i.e. unauthorized access or use of SSA information) SSA records for information not related to an SWA client case (e.g. celebrities, SWA employees, relatives, etc.) If the SWA system design is transaction driven (i.e. employees cannot initiate transactions themselves, rather, the SWA system triggers the transaction to SSA), or if the design includes a "permission module" (i.e. the transaction requesting information from SSA cannot be triggered by an SWA employee unless the SWA system contains a record containing the client's Social Security Number), then the SWA needs only minimal additional monitoring and anomaly detection. If such designs are used, the SWA only needs to monitor any attempts by their employees to obtain information from SSA for clients not in their client system, or attempts to gain access to SSA data within the SWA system by employees not authorized to have access to such information.

If the SWA design does not include either of the security control features described above, then the SWA must develop and implement compensating security controls to prevent their employees from browsing SSA records. These controls must include monitoring and anomaly detection features, either systematic, manual, or a combination thereof. Such features must include the capability to detect anomalies in the volume and/or type of queries requested by individual SWA employees, and systematic or manual procedures for verifying that requests for SSA information are in compliance with valid official business purposes. The SWA system must produce reports providing SWA management and/or supervisors with the capability to appropriately monitor user activity, such as:

- User ID exception reports

  This type of report captures information about users who enter incorrect user ID's when attempting to gain access to the system or to the transaction that initiates requests for information from SSA, including failed attempts to enter a password.

- Inquiry match exception reports

  This type of report captures information about users who may be initiating transactions for Social Security Numbers that have no client case association within the SWA system.

- System error exception reports

This type of report captures information about users who may not understand or be following proper procedures for access to SSA information through the ICON system.

- Inquiry activity statistical reports

This type of report captures information about transaction usage patterns among authorized users, which would provide SWA management a tool for monitoring typical usage patterns compared to extraordinary usage.

The SWA must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors, or to local security officers, to ensure that the reports are used by those whose responsibilities include monitoring the work of the authorized users.

Meeting this Requirement

The SWA must explain in their documentation how their system design will monitor and/or prevent their employees from browsing SSA information. If the design is based on a "permission module" (see above), a similar design, or is transaction driven (i.e. no employee initiated transactions) then the SWA does not need to implement additional systematic and/or managerial oversight procedures to monitor their employees access to SSA information. The SWA only needs to monitor user access control violations. The documentation should clearly explain how the system design will prevent SWA employees from browsing SSA records.

If the SWA system design permits employee initiated transactions that are uncontrolled (i.e. no systematically enforced relationship to an SWA client), then the SWA must develop and document the monitoring and anomaly detection process they will employ to deter their employees from browsing SSA information. The SWA should include sample report formats demonstrating their capability to produce the types of reports described above, and the SWA should include a description of the process that will be used to distribute these reports to managers/supervisors, and the management controls that will ensure the reports are used for their intended purpose.

During onsite certification, the IV&V contractor, or other certifier, will request a demonstration of the SWA's monitoring and anomaly detection capability.

- If the design is based on a permission module or similar design, or is transaction driven, the SWA will demonstrate how the system triggers requests for information from SSA.

- If the design is based on a permission module, the SWA will demonstrate the process by which requests for SSA information are prevented for Social Security Numbers not present in the SWA system (e.g. by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the SWA system.)

11

- If the design is based on systematic and/or managerial monitoring and oversight, the SWA will provide copies of anomaly detection reports and demonstrate the report production capability.

During onsite certification, the IV&V contractor, or other certifier, also will meet with a sample of managers and/or supervisors responsible for monitoring ongoing compliance to assess their level of training to monitor their employee's use of SSA information, and for reviewing reports and taking necessary action.

5. Management Oversight and Quality Assurance

The SWA must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized employees have access to SSA information through the ICON system, and to ensure there is ongoing compliance with the terms of the SWA's data exchange agreement with SSA. The management oversight function must consist of one or more SWA management officials whose job functions include responsibility for assuring that access to and use of SSA information is appropriate for each employee position type for which access is granted.

This function also should include responsibility for assuring that employees granted access to SSA information receive adequate training on the sensitivity of the information, safeguards that must be followed, and the penalties for misuse, and should perform periodic self-reviews to monitor ongoing usage of the online access to SSA information. In addition, there should be the capability to randomly sample work activity involving online requests for SSA information to determine whether the requests comply with these guidelines. These functions should be performed by SWA employees whose job functions are separate from those who request or use information from SSA.

Meeting this Requirement

The SWA must document that they will establish and/or maintain ongoing management oversight and quality assurance capabilities for monitoring the issuance and maintenance of user ID's for online access to SSA information, and oversight and monitoring of the use of SSA information within the SWA business process. The outside entity should describe how these functions will be performed within their organization and identify the individual(s) or component(s) responsible for performing these functions.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individual(s) responsible for these functions and request a description of how these responsibilities will be carried out.

6. Security Awareness and Employee Sanctions

The SWA must establish and/or maintain an ongoing function that is responsible for providing security awareness training for employees that includes information about their

responsibility for proper use and protection of SSA information, and the possible sanctions for misuse. Security awareness training should occur periodically or as needed, and should address the Privacy Act and other Federal and State laws governing use and misuse of protected information. In addition, there should be in place a series of administrative procedures for sanctioning employees who violate these laws through the unlawful disclosure of protected information.

Meeting this Requirement

The SWA must document that they will establish and/or maintain an ongoing function responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse of SSA information. The SWA should describe how these functions will be performed within their organization, identify the individual(s) or component(s) responsible for performing the functions, and submit copies of existing procedures, training material and employee acknowledgment statements.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individuals responsible for these functions and request a description of how these responsibilities are carried out. The IV&V contractor, or other certifier, also will meet with a sample of SWA employees to assess their level of training and understanding of the requirements and potential sanctions applicable to the use and misuse of SSA information.

C. Onsite Systems Security Certification Review

The SWA must obtain and participate in an onsite review and compliance certification of their security infrastructure and implementation of these security requirements prior to being permitted to submit online transaction to SSA through the ICON system. DOL will require an initial onsite systems security certification review to be performed by either an independent IV&V contractor, or other DOL approved certifier. The onsite certification will address each of the requirements described above and will include, where appropriate, a demonstration of the SWA's implementation of each requirement. The review will include a walkthrough of the SWA's data center to observe and document physical security safeguards, a demonstration of the SWA's implementation of online access to SSA information through the ICON system, and discussions with managers/supervisors. The IV&V contractor, or other certifier, also will visit at least one of the SWA's field offices to discuss the online access to SSA information with a sample of line workers and managers to assess their level of training and understanding of the proper use and protection of SSA information.

The IV&V contractor, or other certifier, will separately document and certify SWA compliance with each SSA security requirement. To fully comply with SSA's security requirements and be certified to connect to SSA through the ICON system, the SWA must submit to DOL a complete package of documentation as described above and a complete certification from an independent IV&V contractor, or other DOL approved certifier, that the

SWA system design and infrastructure is in agreement with the SWA documentation and consistent with SSA requirements. Any unresolved or unimplemented security control features must be resolved by the SWA before DOL will authorize their connection to SSA through the ICON system.

Following initial certification and authorization from DOL to connect to SSA through the ICON system, SSA is responsible for future systems security compliance reviews. SSA conducts such reviews approximately once every three years, or as needed if there is a significant change in the SWA's computing platform, or if there is a violation of any of SSA's systems security requirements or an unauthorized disclosure of SSA information by the SWA. The format of those reviews generally consists of reviewing and updating the SWA compliance with the systems security requirements described above.